Et visionært teknologidesign

Jensen, Christian D.

Publication date:
2010

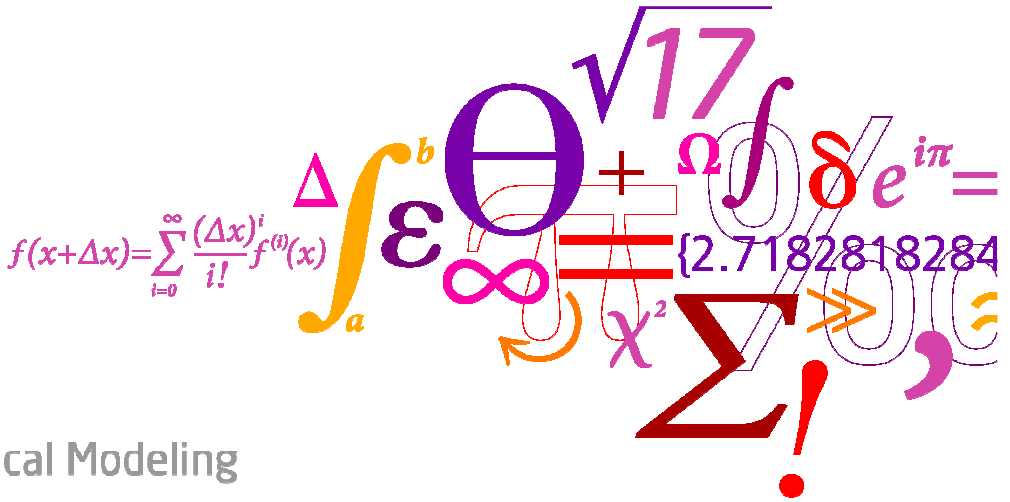
Document Version
Publisher's PDF, also known as Version of record

Et visionært teknologidesign

Christian Damsgaard Jensen

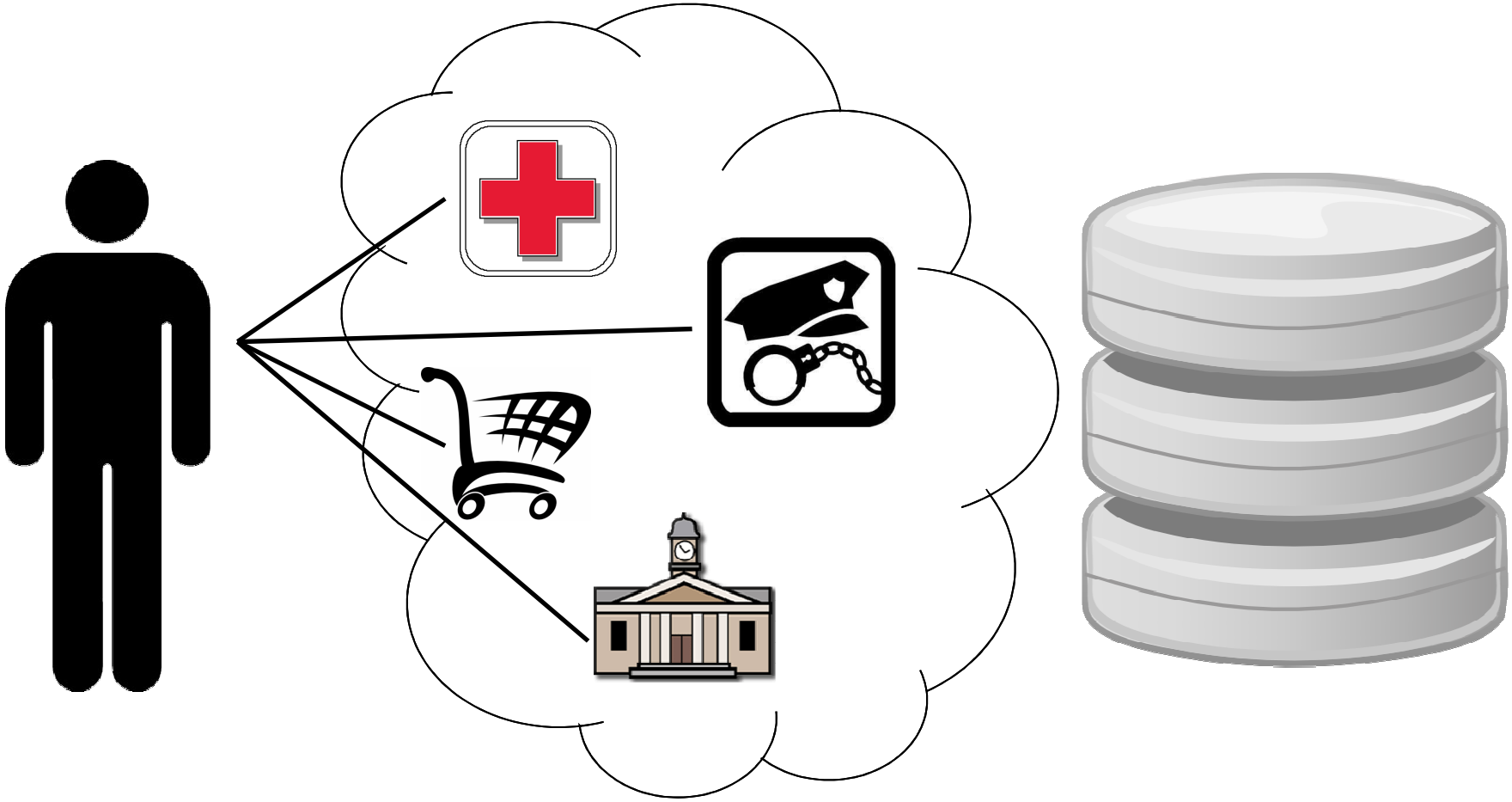
DTU Informatik
Danmarks Tekniske Universitet

Christian.Jensen@imm.dtu.dk



DTU Informatics
Department of Informatics and Mathematical Modeling

Opsamling af personlige data



Privatlivets fred er truet

- Der er et stigende antal rapporter om brud på ”privacy”
  - Indbrud på computer systemer
  - Stigende privat registrering af data
    - Google Streetview, Apple iPhone lokalisering, …
  - Tab af data medier
    - Forlagte CD’er, USB nøgleringe osv.
    - Hard diske i stjålne laptops
  - Stigende antal nationale aftaler om udlevering af data
    - SWIFT, adgang til DNA register fra USA, …
  - Stigende samkøring af registre
    - Gør det svært at vide hvad der er registreret om den enkelte
    - Gør det svært at sikre at data kun benyttes til rette formål
- Eksisterende ”Privacy Enhancing Technologies” fokuserer på teknologi
  - Anonyme eller pseudonyme interaktioner
  - Mangler fokus på operationelle aspekter
    - Hvordan data opbevares, hvem har adgang til data, …

Beskyttelse af privatlivets fred

- Formål
  - Begrænse mængden af personhenførbar information der kan opsamles og kombineres med data fra andre kilder
  - Begrænset af anti-terror lovgivning, skattelovgivning, …
- Operationelle aspekter
  - Privacy Enhancing Technologies
  - Persondata lovgivning
    - National lovgivning
    - EU direktiver
  - Driftmiljø
    - Installation og drift af systemet, uddannelse af personale
    - Fysisk sikkerhed
- Praktisk Privacy vurdering
  - Nødvendigt at inddrage alle aspekter nævnt ovenfor
  - vigtig parameter når nye systemer skal udvikles eller indkøbes
    - En vurdering kan bruges fremadrettet i udviklingsfasen

Operationel privacy vurderings model

- Fokus på risiko for afsløring af personhenførbare informationer
  - Sandsynligheden for en lækage
  - Omkostninger for den enkelte borger i tilfælde af en lækage
    - Ikke alle oplysninger er lige følsomme (patientjournal vs. adresse)
    - Svært at vurdere præcist, så bredde følsomhedsklasser må overvejes
      - Nogle data er naturligt følsomme (helbred, straffeattest, skat, …)
      - Nogle data gør det nemmere at begå identitetstyveri

- Udviklet en model baseret på eksisterende ideer
  - Persondatalovgivning (forskellig fra land til land)
  - Sikkerhedsstandarder (Common Criteria, ISO/IEC 17799, …)
    - Beskriver direkte privacy faktorer
    - Udledning af privacy faktorer baseret på anbefalinger og ”best practises”

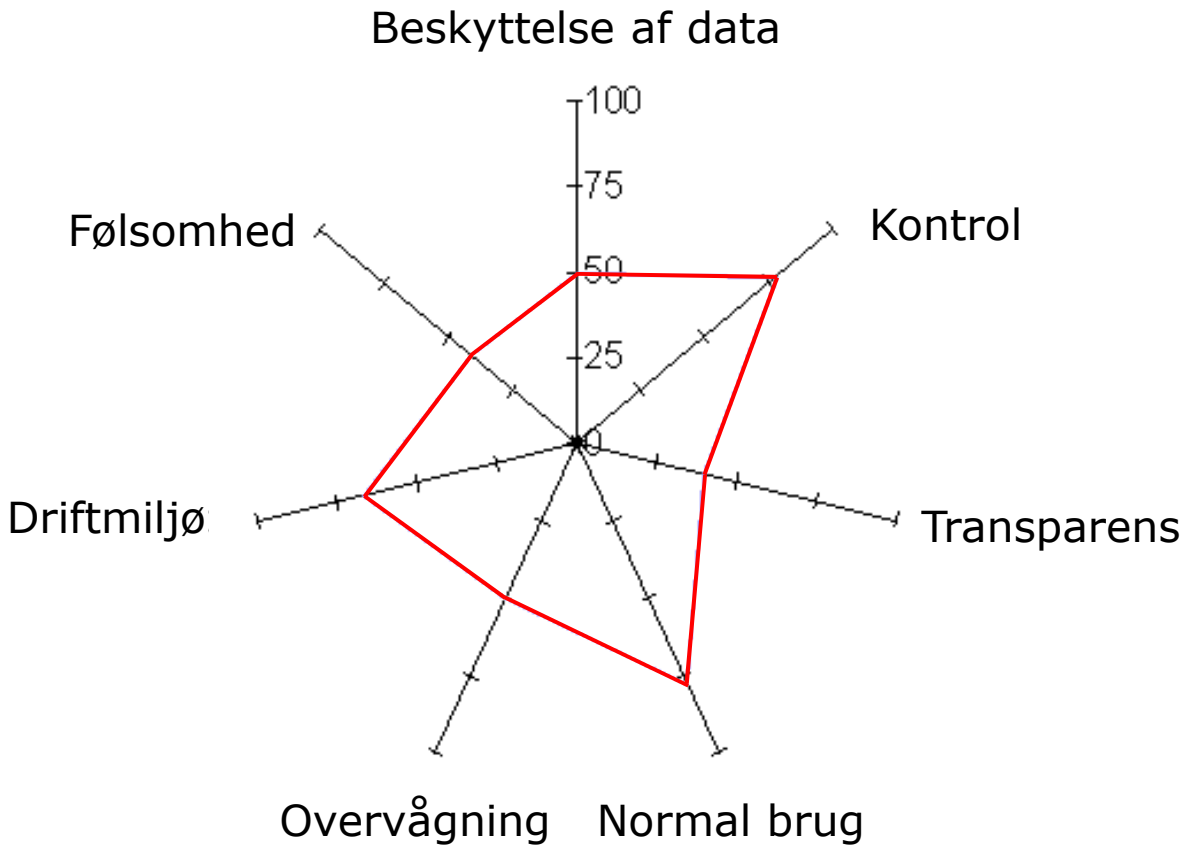
Privacy faktorer

- Beskyttelse af data
  - Risici vedrørende data (lagring i databaser og kommunikation i netværk)
- Følsomhed af data
  - Risici for borgere/brugere som følge af datalækage
- Driftmiljø
  - Risici vedrørende driftmiljøet – fra design af systemet til daglig drift
- Overvågning
  - Risiko for overvågning udført af systemets driftsorganisation
- Normal brug
  - Risici som følge af autoriseret brug af data
- Transparens
  - Information til brugere om registreret data og deres brug
- Kontrol
  - Kontroller der udføres for at undersøge brug og lagring af data (revision)

Måling af privacy faktorer

- Vurdering skal være så objektiv som muligt
  - Der er ingen global definition af privacy, så metode til måling skal virke med de fleste definitioner
- Vurdering skal kunne afspejle løbende ændringer i systemet
  - Forbedringer skal kunne måles
- Vurdering skal tillade sammenligning på tværs af lignende systemer
  - Ønsker at sammenligne forskellige systemer eller designalternativer
    - Der er intet privacy optimum, så systemer må ligne hinanden
- Definerer simple spørgsmål for hver privacy faktor (inkl. undergrupper)
  - Svar for hver undergruppe tildeles point
  - Point fra alle undergrupper samles til en overordnet vurderin
    - Indtil videre foreslår vi et simpelt gennemsnit
- Resultat skal præsenteres simpelt og intuitivt
  - Almindelige mennesker skal kunne vurdere resultatet af målingen
    - Systemplanlæggere og programmører er ikke privacy eksperter

Præsentation af privacy vurdering



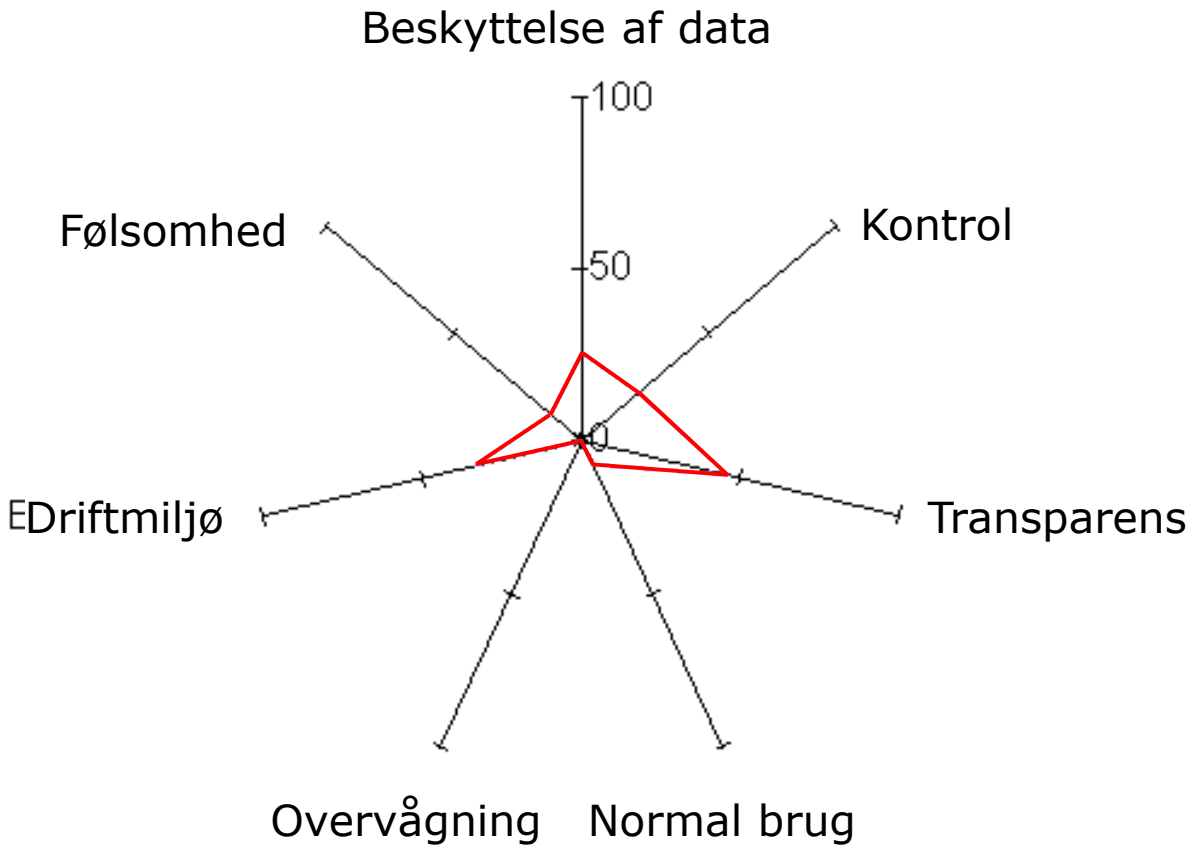
Scenario 1: Mindre patientdatasystem

- Patientjournal
  - Til praktiserende læger og små lægehuse
  - Patientdata er naturligt følsomme
    - Systemet lagrer alt hvad lægen finder relevant at skrive
  - Udviklet af mindre softwarehus til få læger/klinikker
- Data krypteres ikke på hard disk, men kontoret låses udenfor arbejdstid
  - Sikrer en vis grad af fysisk sikkerhed
- CPR nummer bruges som primær nøgle
- Læger kan udskrive patientjournaler til hjemmebesøg og patienter kan tage dem med hjem til nærmere studier
  - Patienter skal selv bede lægen om en kopi
- Læger og sekretærer er ikke specielt uddannet til brug af systemet
- Data indføres ved patientens første konsultation og opdateres løbende
  - Data forældes ikke og der er ingen intern/ekstern revision af systemet

Vurdering af scenario 1

- Beskyttelse af data
  - Basal beskyttelse, men ingen kryptering af data [25%]
- Følsomhed af data
  - Naturligt følsomme data, ingen id-separation [12%]
- Driftmiljø
  - Lukket miljø, ingen ekstern revision [33%]
- Overvågning
  - Ubegrænset adgang til data, nøgle er nemt tilgængelig [0%]
- Normal brug
  - Ingen uddannelse af personale, ingen adgangskontrolsystem, data kan nemt eksporteret (udskrives) [8%]
- Transparens
  - Brugere kan få adgang til data, men de må bede eksplicit om den [46%]
- Kontrol
  - Ingen revision, ingen brugerkontrol over hvad der registreres [22%]

Præsentation af vurdering af Scenario 1



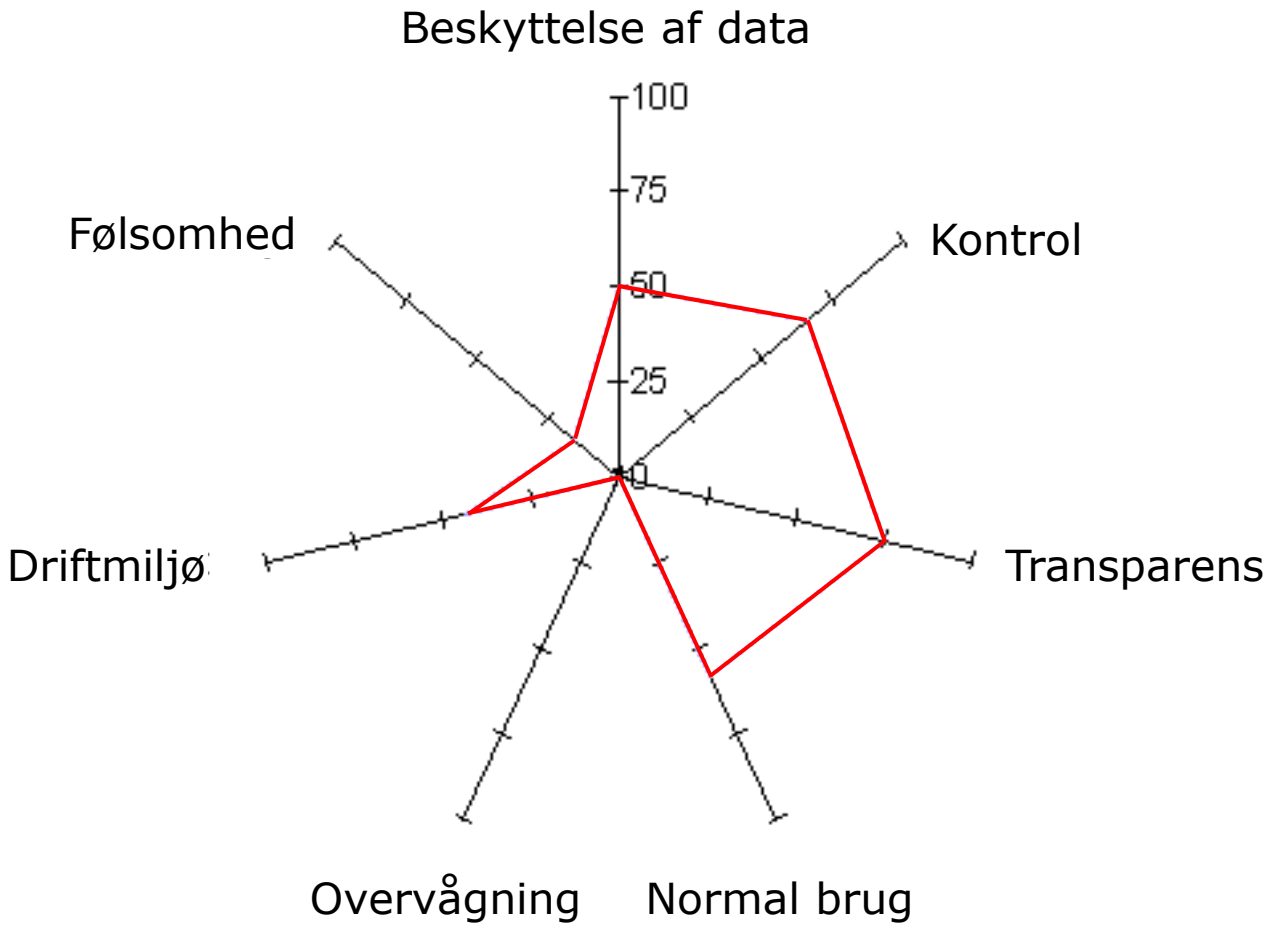
Scenario 2: Større patientdatasystem

- System der minder om Scenario 1
- Udviklet af IT-sektionen af et større medicinalfirma
  - Medicinalfirmaet vedligeholder centrale databaseservere i egne serverrum
  - Lagre data i sikrede serverrum, datakommunikation er krypteret
- Systemet er kædet sammen med lokale hospitaler og patienter har adgang til at se registrerede data på nettet
  - Patienter kan anmode om at få rettet forkerte/overflødige data
- CPR nummer bruges som primær nøgle
- Systemet lagrer alt hvad lægen finder relevant at skrive
- Særligt kursus til læger, sygeplejersker og administrativt personale
- Systemet sammenligner ”offentlige” data med andre offentlige systemer
  - Adresser, telefonnummer, …
- Systemet revideres periodisk af eksterne autoriserede IT-revisorer

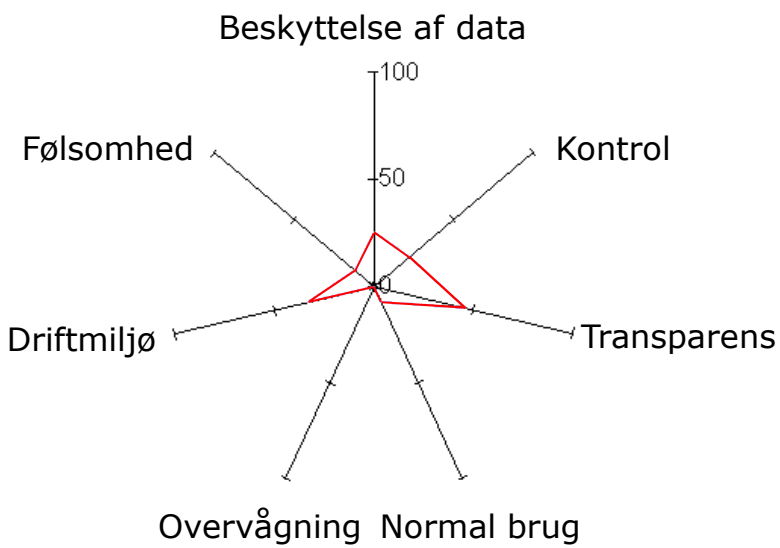
Vurdering af scenario 2

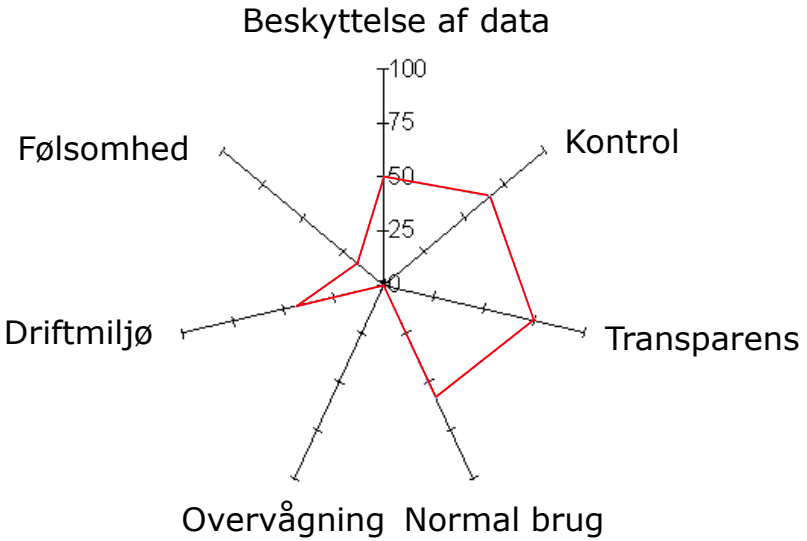
- Beskyttelse af data
  - Fysisk beskyttelse af lagrede data og krypteret kommunikation [50%]
- Følsomhed af data
  - Naturligt følsomme data, mulighed for id-separation [16%]
- Driftmiljø
  - Ekstern gennemgang af kode, overholder gældende lovgivning [44%]
- Overvågning
  - Ubegrænset adgang til data, nøgle er nemt tilgængelig [0%]
- Normal brug
  - Uddannelse af personale, rollebaseret adgangskontrol, data kan stadig nemt eksporteret (udskrives) [58%]
- Transparens
  - Brugere har nem adgang til data (online) [75%]
- Kontrol
  - Ekstern revision, ingen brugerkontrol over hvad der registreres [66%]

Præsentation af vurdering af Scenario 2



Sammenligning af de to evalueringer





- Patientdata er naturligt følsomme, så begge systemer scorer lavt
  - Følsomhed af data og overvågning er de primære områder at forbedre
- Hovedparten af øvrige faktorer er bedre i system 2, der blev udviklet af et større firma med flere ressourcer
  - Især fremhæves ekstern kodegennemgang, uddannelse og revision
- Større areal af figuren indikerer bedre privacy

Konklusioner

- Privatlivets fred er subjektiv, så det er vigtigt at en vurdering af privacy udføres med objektive kriterier
- Operationel privacy model baseret på 7 faktorer
  - Hver faktor opnår en score der reflekterer den samlede vurdering af alle delelementer i den givne faktor
  - Faktorer og undergrupper overlapper med hinanden fordi vi vil hellere måle en faktor flere gange (i forskellig sammenhæng) end glemme noget
  - Modeller hjælper systemudviklere med at vurdere deres design, IT-chefer med beslutninger vedrørende indkøb og brugere med at vælge den rette leverandør af en efterspurgt tjeneste
- Modellen er afprøvet på nogle virkelige systemer og resultaterne virker lovende
  - Evaluering af flere systemer (evt. en hel branche) vil kunne bekræfte dette resultat og hjælpe med at forfine modellen.
- En videreudvikling af modellen kunne måske danne grundlag for certificering